# 可验证第三方的量子秘密信息平等互换协议 *

邵婷婷，张仕斌[†]，昌 燕

(成都信息工程大学 网络空间安全学院，成都 610225)

**摘 要：**为了实现通信双方的信息交换，提出一种可验证第三方的量子秘密信息平等互换协议。该协议中，由第三方制备 GHZ 态，将其中的两个粒子分别发送给通信的双方。通信双方分别对收到的粒子进行泡利操作，然后发送给第三方；第三方对新的 GHZ 态进行测量并公布测量结果，通信双方根据公布的测量结果能够推测出对方的秘密信息。通过分析可知，该协议能够实现通信双方秘密信息的平等互换，可以对第三方的身份进行认证，第三方负责进行粒子的分发和测量，但不能获得秘密信息。该协议能够检测窃听，同时能够抵御截获重发攻击、中间人攻击和参与者攻击。

**关键词：**量子通信；秘密信息；GHZ 态；平等互换；可验证第三方

**中图分类号：**TN915.08 doi: 10.19734/j.issn.1001-3695.2018.07.0560

## Third party verifiable quantum secret information equal exchange protocol

Shao Tingting, Zhang Shibin[†], Chang Yan

(*School of Cybersecurity, Chengdu University of Information Technology University, Chengdu 610225, China*)

**Abstract:** In order to realize the information exchange between the two parties, the paper proposes a verifiable third party quantum secret information equal exchange protocol. In this protocol, a third party prepares the GHZ state and sends the particles to each communicating parties respectively. The two parties of the communication respectively conduct the pauli operation on the received particles and then send them to a third party. A third party measures the new GHZ state and publishes the results. Both parties can deduce the other party's secret information according to the published measurement results. Through analysis, this protocol can realize the equal exchange of secret information between the two parties, and can verify the identity of the third party. The third party is responsible for the distribution and measurement of particles but cannot obtain secret information. Analysis shows that the protocol can detect eavesdropping. At the same time, the protocol can resist the interception and retransmission attack, man-in-the-middle attack and participant attack.

**Key words:** quantum communication; secret information; GHZ state; equal exchange; verifiable third party



## 0 引言

随着时间的发展，经典的密码体制已经比较完善，并且被广泛的应用在各个生活领域，保护着人们的信息安全。但是，随着量子算法[1,2]和量子计算机研制[3]的提出，经典密码系统的安全性受到极大的挑战。1969 年 Wiesner 首先提出用量子效应保护信息，他写了一篇《共轭编码》[4]的论文。量子通信具有两个基本的特征：无条件安全性及对窃听的可检测性。无条件的安全性是指在攻击者拥有无限的计算资源前提下仍然不可以破译该密码系统。对窃听的可检测性是指通信中的用户之间信道受到干扰时，根据测不准原理可以检测出干扰的存在。近年来，量子通信取得了一系列可喜可贺的研究成果[5,6]，主要包括量子密钥分发(QKD)[7,8]，量子秘密共享(QSS)[9,10]，量子隐私查询(QPQ)[11,12]，量子安全直接通信(QSDC)[13,14]等。

现实生活中，如果两个用户各自拥有一条秘密信息，用户 1 想要获得用户 2 的秘密信息，同时用户 2 想要获得用户 1 的秘密信息，两个用户可以通过秘密信息的交换获得更多的信息。但是在信息交换的过程中，以往的通信协议通常是用户 1 首先发送秘密信息给用户 2，用户 2 确认收到秘密信息之后，才将自己的秘密信息发送给用户 1。这种秘密信息交换的方式存在风险，有可能用户 2 获得用户 1 的秘密信息，却欺骗用户 1，发送假的秘密信息给用户 1。用户 1 获得的是假的秘密信息，但是自己的秘密信息已经泄露给用户 2。为了避免这种风险的存在，本文设计了一种新的可验证第三方的量子秘密信息平等互换协议。

本协议首先由第三方制备 GHZ 态，将其中的两个粒子分别发送给通信双方。虽然协议中引入了第三方，但是可以对第三方的身份进行验证，减少对第三方的依赖。收到粒子后的通信双方利用泡利操作将秘密信息分别加载到粒子上，再返回给第三方，通信双方对新的 GHZ 态进行测量并公布测量结果。通信双方可以根据公布的测量结果推测出对方的秘密信息。该协议可以使通信的双方同时获得对方的秘密信息，实现秘密信息的平等互换，避免秘密信息交换过程中一方欺骗另一方的情况。通过分析可知，第三方的身份可以被验证，能够确保第三方是安全可信的，同时，该协议在实现过程中能够进行检测窃听，抵御截获重发攻击、中间人攻击和参与者攻击。

**收稿日期：**2018-07-18；**修回日期：**2018-09-07 **基金项目：**国家重点研发计划资助项目（2017YEB0802302）；国家自然科学基金资助项目（61572086，61402085）；四川省高校科研创新团队项目（17TD0009）；四川省学术和技术带头人培养支持经费资助项（2016120080102643）；四川省应用基础资助项目（2017JY0168）；四川省重点研发计划项目（2018TJPT0012）

**作者简介：**邵婷婷（1991-），山东成武人，硕士研究生，主要研究方向为量子安全通信；张仕斌（1971-），男（通信作者），教授，博士，主要研究方向为量子密码学、网络空间安全（cuitzsb@cuit.edu.cn）；昌燕（1979-），女，副教授，博士，主要研究方向为量子密码学.

## 1　基本原理

四种泡利矩阵如下：

$$\left.\begin{array}{l}\sigma_{00}=\begin{bmatrix}1&0\\0&1\end{bmatrix},\ \sigma_{10}=\begin{bmatrix}0&-1\\1&0\end{bmatrix}\\ \sigma_{01}=\begin{bmatrix}0&1\\1&0\end{bmatrix},\ \sigma_{11}=\begin{bmatrix}1&0\\0&-1\end{bmatrix}\end{array}\right\} \tag{1}$$

对 $|0\rangle$ 和 $|1\rangle$ 执行四种泡利操作得到如下结果：

$$\begin{array}{ll}\sigma_{00}|0\rangle=|0\rangle, & \sigma_{00}|0\rangle=|1\rangle\\ \sigma_{01}|0\rangle=|1\rangle, & \sigma_{01}|0\rangle=|0\rangle\\ \sigma_{10}|0\rangle=|1\rangle, & \sigma_{10}|0\rangle=-|0\rangle\\ \sigma_{11}|0\rangle=|0\rangle, & \sigma_{11}|0\rangle=-|1\rangle\end{array} \tag{2}$$

8 种 GHZ 态如下：

$$\left.\begin{array}{ll}|\Psi\rangle_a=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{123} & |\Psi\rangle_b=\frac{1}{\sqrt{2}}(|000\rangle-|111\rangle)_{123}\\ |\Psi\rangle_c=\frac{1}{\sqrt{2}}(|001\rangle+|110\rangle)_{123} & |\Psi\rangle_d=\frac{1}{\sqrt{2}}(|001\rangle-|110\rangle)_{123}\\ |\Psi\rangle_e=\frac{1}{\sqrt{2}}(|010\rangle+|101\rangle)_{123} & |\Psi\rangle_f=\frac{1}{\sqrt{2}}(|010\rangle-|101\rangle)_{123}\\ |\Psi\rangle_g=\frac{1}{\sqrt{2}}(|011\rangle+|100\rangle)_{123} & |\Psi\rangle_h=\frac{1}{\sqrt{2}}(|011\rangle-|100\rangle)_{123}\end{array}\right\} \tag{3}$$

纠缠态 $|\Psi\rangle_a=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{123}$ 在 X 基下的表示如下：

$$|\Psi\rangle_a=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{123}=\frac{1}{2}(|+++\rangle+|+--\rangle+|-+-\rangle+|--+\rangle)_{123} \tag{4}$$

由式（4）可知，纠缠态 $|\Psi\rangle_a=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{123}$ 中的三个粒子有如下关系：当第一个粒子为态 $|+\rangle$ 时，第二个和第三个粒子状态相同；当第一个粒子为 $|-\rangle$ 态时，第二个和第三个粒子状态相反。根据这个特性可以验证一个纠缠态是否是 $|\Psi\rangle_a$ 态。

## 2　协议描述

Alice 拥有秘密信息 $X(x_1,x_2\ldots\ldots x_n)$，Bob 拥有秘密信息 $Y(y_1,y_2\ldots\ldots y_n)$，其中每个 $x_i$ 与 $y_i$ 对应两位二进制比特。Alice 和 Bob 想要进行秘密信息的交换，协议如下：

a）Alice 和 Bob 告知第三方，由第三方制备 m+n 对 $|\Psi\rangle_a=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{123}$ 态，将所有的 1 粒子组成序列 $S_1$；所有的 2 粒子组成序列 $S_2$；所有的 3 粒子组成序列 $S_3$。第三方将序列 $S_1$ 自己保留，在序列 $S_2$ 和序列 $S_3$ 中随机插入诱骗粒子 $|0\rangle$、$|1\rangle$、$|+\rangle$、$|-\rangle$，然后分别发送给 Alice 和 Bob。

b)Alice 和 Bob 收到第三方发送的粒子后进行窃听检测，第三方公布诱骗粒子的位置及对应的测量基，如果插入的是 $|0\rangle$ 或 $|1\rangle$ 则公布 Z 基，如果插入的是 $|+\rangle$ 或 $|-\rangle$ 则公布 X 基。Alice 和 Bob 将对应位置的粒子提取出来用 X 基或 Z 基测量。若测量结果错误高于阈值，则放弃通信，否则进行 c）步。

c）对第三方的身份进行认证，Alice 和 Bob 随机指定 m 个粒子及对应粒子的位置，要求第三方用 X 基进行测量并用经典信道公布测量结果，Alice 和 Bob 收到测量结果之后也用 X 基测量对应位置的粒子。如果第三方正确制备了 GHZ 态，应该满足第三方公布 $|+\rangle$ 态时，Alice 和 Bob 的测量结果相同；第三方公布 $|-\rangle$ 态时，Alice 和 Bob 的测量结果相反。如果验证第三方准确制备了 GHZ 态，则进行 d）步。

d）Alice 根据自己的秘密信息 $X$ 对 n 个粒子执行四种泡利操作，如果 $x_i$ 为 00 则执行 $\sigma_{00}$ 操作；如果 $x_i$ 为 01 则执行 $\sigma_{01}$ 操作；如果 $x_i$ 为 10 则执行 $\sigma_{10}$ 操作；如果 $x_i$ 为 11 则执行 $\sigma_{11}$ 操作。Alice 执行泡利操作之后形成新的序列 $S_2^{'}$，同理，Bob 根据自己的秘密信息 Y 执行泡利操作之后形成新的序列 $S_3^{'}$。Alice 在序列 $S_2^{'}$ 中随机插入诱骗粒子 $|0\rangle$、$|1\rangle$、$|+\rangle$、$|-\rangle$，然后发送给第三方，同理，Bob 把随机插入诱骗粒子的 $S_3^{'}$ 也发送给第三方。

e）第三方收到 Alice 和 Bob 发来的粒子之后，Alice 和 Bob 分别公布诱骗粒子的位置及测量基，同 b）步第三方公布的方式相同。

f）第三方取出诱骗粒子之后得到 $S_2^{'}$ 和 $S_3^{'}$，然后与自己的序列 $S_1$ 联合测量，测量结果如表 1 所示，第三方公布测量的 GHZ 态。

g）Alice 根据表 1 第三方公布的测量结果可以推测出信息 $Y^{'}$，同理，Bob 根据第三方公布的测量结果可以推测出信息 $X^{'}$。Alice 用经典信道公布 $Y^{'}$ 异或 $X$ 的结果，Bob 用经典信道公布 $X^{'}$ 异或 $Y$ 的结果，如果两者公布的内容相同，说明第三方没有存在欺骗，Alice 得到 Bob 的秘密信息 $Y$，Bob 得到 Alice 的秘密信息 $X$。

表 1　泡利操作后 GHZ 态的测量结果

Table 1　Measurement results of GHZ state after Pauli operation

| Alice | Bob | | | |
|---|---|---|---|---|
| | $\sigma_{00}$ | $\sigma_{01}$ | $\sigma_{10}$ | $\sigma_{11}$ |
| $\sigma_{00}$ | $\|\Psi\rangle_a$ | $\|\Psi\rangle_c$ | $\|\Psi\rangle_d$ | $\|\Psi\rangle_b$ |
| $\sigma_{01}$ | $\|\Psi\rangle_e$ | $\|\Psi\rangle_g$ | $\|\Psi\rangle_h$ | $\|\Psi\rangle_f$ |
| $\sigma_{10}$ | $\|\Psi\rangle_f$ | $\|\Psi\rangle_h$ | $\|\Psi\rangle_g$ | $\|\Psi\rangle_e$ |
| $\sigma_{11}$ | $\|\Psi\rangle_b$ | $\|\Psi\rangle_d$ | $\|\Psi\rangle_c$ | $\|\Psi\rangle_a$ |

## 3　协议分析

### 3.1　协议的正确性分析

如果通信的双方 Alice 和 Bob 想要进行秘密信息的交换，由第三方制备 GHZ 态 $|\Psi\rangle_a=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{123}$，将粒子 2 发送给 Alice，将粒子 3 发送给 Bob。Alice 和 Bob 根据秘密信息对粒子进行泡利操作，然后发送给第三方，第三方将返回的粒子与自己手中的粒子进行测量并公布测量结果。如表 1，Alice 根据第三方公布的测量结果及自己的秘密信息能够推测出 Bob 的秘密信息，同理，Bob 也能推测出 Alice 的秘密信息。协议的简化流程图如图 1 所示。

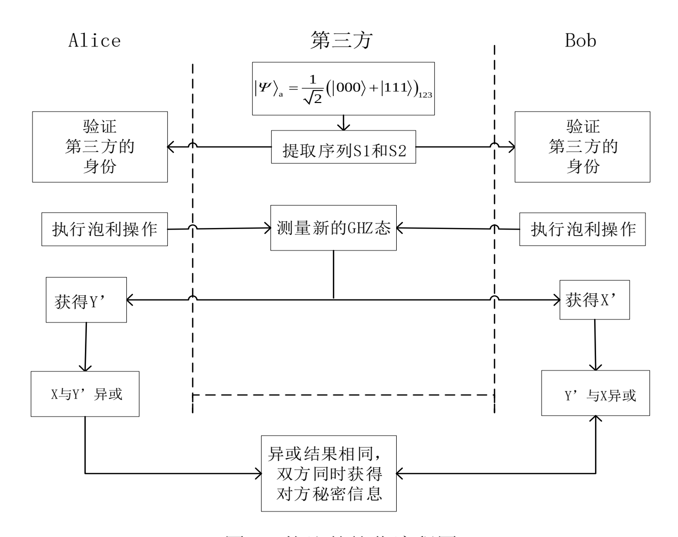



图 1　协议的简化流程图

Fig. 1　Protocol simplified flow chart

协议举例：假设 Alice 拥有秘密信息 001011，Bob 拥有秘密信息 110011。Alice 和 Bob 告知第三方，由第三方制备 m+n 对 $|\Psi\rangle_a = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{123}$ 态，将所有的 2 粒子随机插入诱骗粒子后发送给 Alice，将所有的 3 粒子随机插入诱骗粒子后发送给 Bob。Alice 和 Bob 收到第三方发送的粒子后进行窃听检测，证明信道安全之后对第三方的身份进行验证。 Alice 和 Bob 随机指定粒子的位置，要求第三方用 X 基进行测量，当第三方公布的是 $|+\rangle$ 态时，Alice 和 Bob 用 X 基测量的测量结果相同。当第三方公布的是 $|-\rangle$ 态时，Alice 和 Bob 用 X 基测量的测量结果相反。验证第三方正确制备 GHZ 态之后，Alice 和 Bob 分别将秘密信息加载到各自的粒子上。Alice 对 2 粒子分别执行 $\sigma_{00}$、$\sigma_{10}$、$\sigma_{11}$ 操作；Bob 对 3 粒子分别执行 $\sigma_{11}$、$\sigma_{00}$、$\sigma_{11}$ 操作。Alice 和 Bob 将执行泡利操作之后的粒子插入诱骗粒子之后发送给第三方。第三方收到粒子，检测窃听之后将诱骗粒子提取出来，联合所有的粒子 1 进行 GHZ 测量。公布测量结果 $|\Psi\rangle_b$ $|\Psi\rangle_d$ $|\Psi\rangle_a$，根据表 1 泡利操作后 GHZ 态的测量结果，Alice 获得信息 110011，Bob 获得信息 001011。Alice 将得到的信息 110011 与自己的秘密信息 001011 异或得 111000 并用经典信道公布；Bob 将得到的信息 001011 与自己的秘密信息 110011 异或得 111000 也用经典信道公布，Alice 和 Bob 公布的信息相同，说明没有存在欺骗或者攻击，Alice 和 Bob 实现秘密信息的平等互换。

## 3.2 安全分析模型的建立

量子秘密信息平等互换协议实现的是两个用户安全的进行信息交换。如图 2 所示，在秘密信息的交换过程中，秘密信息交换面临的攻击者可能有第三方的攻击（包括制备错误的 GHZ 态和公布假的信号）、通信过程中的中间人攻击或截获重发攻击、参与者攻击。

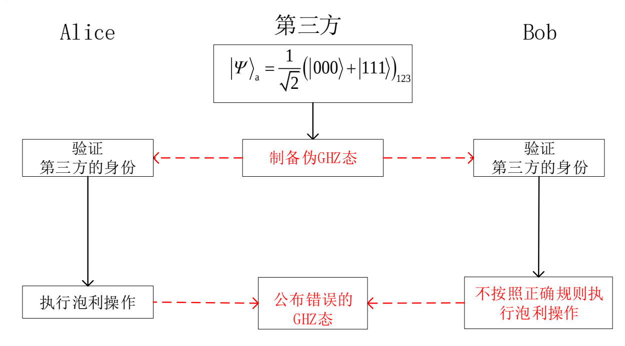



图 2 存在攻击的协议流程图

Fig. 2 Protocol flow chart of the attack process

### 3.2.1 第三方攻击

本协议中，需要第三方做两件事，第一：正确制备 GHZ 态；第二：Alice 和 Bob 执行泡利操作之后返回给第三方，第三方正确公布联合测量的 GHZ 态的结果。

第三方制备 $|\Psi\rangle_a = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{123}$ 态并将粒子 2 和粒子 3 分发给 Alice 和 Bob，假如第三方试图制备假的 GHZ 态，破坏 Alice 和 Bob 的秘密信息交换，将会在验证第三方身份的过程中被发现。在协议的实现过程，需要对第三方进行认证，Alice 和 Bob 分别收到 2 粒子和 3 粒子之后随机选取部分粒子进行验证。要求第三方用 X 基进行测量并用经典信道公布测量结果，Alice 和 Bob 收到测量结果之后也用 X 基测量对应位置的粒子，如果第三方公布 $|+\rangle$ 态，Alice 和 Bob 的测量结果相同；如果第三方公布 $|-\rangle$ 态，Alice 和 Bob 的测量结果相反。满足上述关系，则说明第三方正确制备了 GHZ 态，否则第三方可能存在欺骗。

如果第三方想阻止 Alice 和 Bob 之间的秘密信息交换，采用假信号攻击，将 $S_2'$ 和 $S_3'$ 与自己的序列 $S_1$ 联合测量之后公布假的 GHZ 态，试图使 Alice 得到假的秘密信息 $Y'$，同理，Bob 得到假的秘密信息 $X'$。Alice 根据第三方公布的测量结果推测出信息 $Y'$，同理，Bob 根据第三方公布的测量结果可以推测出信息 $X'$。如果 $Y'$ 与 $Y$ 不相同，$X'$ 与 $X$ 不相同，Alice 和 Bob 分别用经典信道公布 $Y'$ 异或 $X$ 的结果和 $X'$ 异或 $Y$ 的结果将会不同，Alice 和 Bob 将会发现第三方可能公布了假信息，但是第三方不能准确获得 Alice 和 Bob 的消息。例如第三方得到表 1 中的 $|\Psi\rangle_a$ 态，但是并不知道 Alice 和 Bob 的泡利操作是 00 还是 11，二进制比特的数量越多，第三方获得正确消息的概率越小。

### 3.2.2 中间人攻击或截获重发攻击

当信道不安全时，可能存在中间人攻击或截获重发攻击。Alice 和 Bob 收到粒子之后，需要进行信道安全性检测，第三方公布诱骗粒子的位置。Alice 和 Bob 将对应位置的粒子提取出来用 X 基或 Z 基测量并公布测量结果，攻击者一旦选错测量基，就会对粒子造成干扰，如果与第三方插入的诱骗粒子状态不同，则说明可能存在中间人攻击或截获重发攻击，第三方重新发送新的 GHZ 态。Alice 和 Bob 执行泡利操作之后返回给第三方的过程同样需要窃听检测，Alice 和 Bob 也可以通过公布的 $Y'$ 异或 $X$ 与 $X'$ 异或 $Y$ 的结果是否相同判断是否存在攻击者，如果存在攻击者，那么 Alice 通过第三方公布的 GHZ 态获得信息 $Y'$ 并不是 Bob 的真正秘密信息 $Y$，同理，Bob 获得信息 $X'$ 不是 Alice 的真正秘密信息 $X$，因此 $Y'$ 异或 $X$ 与 $X'$ 异或 $Y$ 的结果将会不同。分析可知，本协议可以有效的抵御中间人攻击或截获重发攻击。

### 3.2.3 参与者攻击

假设通信过程中 Bob 试图欺骗 Alice，Bob 不按照正确的秘密信息 $Y$ 执行泡利操作。例如 Alice 的秘密信息是“01”，Bob 的秘密信息是“00”，但是 Bob 却对收到的粒子执行 $\sigma_{11}$ 操作，试图骗取 Alice 的秘密信息。Alice 和 Bob 将执行泡利操作之后的粒子返回给第三方，第三方测量之后公布 $|\Psi\rangle_f$（如果 Bob 正确执行泡利操作应该公布的是 $|\Psi\rangle_e$），Bob 根据自己的秘密信息“00”和表 1 中对应的 $|\Psi\rangle_f$ 得到“10”，而 Alice 的秘密信息是“01”，Bob 并不能通过这种攻击方法获得 Alice 的秘密信息。

## 4 结束语

本文提出一种可验证第三方的量子秘密信息平等互换协议，可以实现通信双方平等的秘密信息交换。本协议可以防止一方欺骗一方获得秘密信息，通信的双方通过第三方公布的消息同时获得对方的秘密信息。本协议可以验证第三方，减少了对第三方的依赖，同时可以抵御中间人攻击或截获重发攻击以及参与者攻击，确保信息的安全平等互换。

## 参考文献：

[1] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring [C]// Proc of the 35th Annual Symposium on the Foundations of Computer Science.Washington DC: IEEE Computer Society, 1994: 124-134.

[2] Grover L K. A fast quantum mechanical algorithm for database search [C]//Proc of the 28th ACM Symposium on Theory of Computing. New York: ACM Press, 1996: 212-219.

[3] Ladd T D, Jelezko F, Laflamme R, *et al*. Quantum computers [J].

Nature, 2010, 464(7285): 45-53.

[4] Wiesner S. Conjugate coding [J]. ACM SIGACT News, 1983, 15(1): 78-88.

[5] Gao Fei, Liu Bin, Wen Qiaoyan. Quantum position verification in bounded-attack-frequencymodel [J]. Science China :Physics, Mechanics & Astronomy, 2016, 59(11): 110311.

[6] Song Xueke, Zhang Hao, Ai Qing, *et al*. Shortcuts to adiabatic holonomic quantum computation in decoherence-free subspace with transitionless quantum driving algorithm [J]. New Journal of Physics, 2016, 18(2): 569-577.

[7] Curty M, Xu Feihu, Cui Wei, *et al*. Finite-key analysis for measurement-device-independent quantum key distribution [J]. Nature Communications, 2014, 5(4): 643-648.

[8] Wang Chao, Wang Shuang, Yin Zhenqian, *et al*. Experimental measurement-device-independent quantum key distribution with uncharacterized encoding [J]. Optics Letters, 2016, 41(23): 5596-5599.

[9] Qin Huawang, Dai Yuewei. Verifiable ($t$,$n$) threshold quantum secret sharing using $d$-dimensional Bell state [J]. Information Processing Letters, 2016, 116(5): 351-355.

[10] Gao Gan. Secure multiparty quantum secret sharing with the collective eavesdropping-check character [J]. Quantum Information Processing, 2013, 12(1): 55-68.

[11] Gao Fei, Liu Bin, Huang Wei, *et al*. Postprocessing of the oblivious key in quantum private query [J]. IEEE Journal of Selected Topics in Quantum Electronics, 2014, 21 (3): 98-108.

[12] Wei Chunyan, Wang Tianyin, Gao Fei. Practical quantum private query with better performance in resisting joint-measurement attack [J]. Physical Review A, 2016, 93(4): 042318-042324.

[13] Patwardhan S, Moulick S R, Panigrahi P K. Efficient controlled quantum secure direct communication protocols [J]. International Journal of Theoretical Physics, 2016, 55(7): 3280-3288.

[14] Cao Zhengwen, Song Dan, Peng Jinye, *et al*. High security quantum secure direct communication protocol based on three-particle GHZ states [C]//Proc of IEEE, International Conference on Nanotechnology. Piscataway, NJ: IEEE Press, 2017: 40-43.